

-2-

IN THE CLAIMS

1. (Currently Amended) A method for detecting modifications to risk assessment scanning caused by an intermediate device, comprising:
  - (a) initiating a risk assessment scan on a target from a remote source utilizing a network;
  - (b) determining whether the risk assessment scan on the target involves an intermediate device coupled between the target and the remote source;
  - (c) receiving results of the risk assessment scan from the target utilizing the network; and
  - (d) notifying an administrator if it is determined that the risk assessment scan on the target involves the intermediate device, wherein additional operations are carried out to improve a risk assessment on the target in view of the presence of the intermediate device coupled between the target and the remote source.
2. (Original) The method as recited in claim 1, wherein the intermediate device includes a router.
3. (Original) The method as recited in claim 1, wherein a plurality of procedures are utilized to determine whether the risk assessment scan involves the intermediate device.
4. (Original) The method as recited in claim 3, wherein at least one of the procedures includes determining a port list associated with the risk assessment scan.
5. (Original) The method as recited in claim 4, wherein the at least one of the procedures further includes determining whether a value of a flag is different for communication attempts using at least two ports on the port list.

-3-

6. (Original) The method as recited in claim 5, wherein the flag includes an ip\_ttl flag.
7. (Original) The method as recited in claim 5, wherein the flag includes a tcp\_win flag.
8. (Original) The method as recited in claim 5, wherein the communications include connection attempts between the remote source and the target utilizing the network.
9. (Original) The method as recited in claim 5, wherein the at least one of the procedures further includes indicating that the risk assessment scan involves the intermediate device if the value of the flag is different for the communication attempts using the at least two ports on the port list.
10. (Original) The method as recited in claim 3, wherein at least one of the procedures includes transmitting a first request for content to the target utilizing the network, and transmitting a second request for a cached version of the content to the target utilizing the network.
11. (Original) The method as recited in claim 10, wherein the cached content is requested from the target utilizing a via tag.
12. (Original) The method as recited in claim 10, wherein the at least one of the procedures further includes analyzing responses to the first and second requests.
13. (Original) The method as recited in claim 12, wherein the at least one of the procedures further includes indicating that the risk assessment scan involves the intermediate device based on the analysis.

-4-

14. (Original) The method as recited in claim 13, wherein the at least one of the procedures further includes indicating that the risk assessment scan involves the intermediate device if the responses to the requests are different.
15. (Original) The method as recited in claim 3, wherein at least one of the procedures includes transmitting a request without specifying a host header value.
16. (Original) The method as recited in claim 15, wherein the at least one of the

PAGE 7/7 \* RCVD AT 3/30/2005 7:39:06 PM [Eastern Standard Time] \* SVR:USPTO-EFXRF-1/0 \* DNS:8729306 \* CSID:408 971 4660 \* DURATION (mm-ss):02-06

BEST AVAILABLE COPY